# THÉORIE DES FONCTIONS NUMÉRIQUES SIMPLEMENT PÉRIODIQUES.

PAR EDOUARD LUCAS, *Professeur au Lycée Charlemagne, Paris.*

(Voir pag. 240 et suiv.)

## SECTION XXIV.

*De l'apparition des nombres premiers dans les séries récurrentes de première espèce.*

Dans les séries récurrentes de première espèce, $a$ et $b$ désignent deux nombres entiers, positifs et premiers entre eux; il est d'abord évident que les diviseurs premiers de $a$ et de $b$, ou de $Q = ab$, ne se trouvent jamais comme facteurs dans la série; il ne sera pas tenu compte de ces diviseurs dans tout ce qui va suivre. On déduit immédiatement de la première des formules (4), la démonstration du théorème de FERMAT. En effet, on a, en négligeant les multiples de $p$, supposé premier et impair,

$$2^{p-1}\frac{a^p - b^p}{a - b} \equiv \delta^{p-1}, \text{ (Mod. } p) \,.$$

Multiplions les deux termes de la congruence par $\delta = a - b$, nous obtenons

$$2^{p-1}(a^p - b^p) \equiv (a - b)^p, \text{ (Mod. } p) \,;$$

supposons $a - b = 2$, et divisons par $2^{p-1}$, il vient

$$a^p - b^p \equiv a - b, \text{ (Mod. } p) \,,$$

ou, encore

$$a^p - a \equiv b^p - b, \text{ (Mod. } p) \,.$$

Ainsi, le reste de la division de $a^p - a$, par $p$ premier, ne change pas lorsque l'on diminue $a$ de deux unités, et par suite de 2, 4, 6, 8, . . . unités; mais pour $a = 0$ ou $a = 1$, ce reste est nul; donc $a^p - a$ est toujours divisible par le nombre premier $p$, quelque soit l'entier $a$. Par suite, si le nombre entier $a$ n'est pas divisible par $p$, la différence $a^{p-1} - 1$ est divisible par $p$; c'est précisément l'énoncé du théorème en question.

En supposant maintenant $a$ et $b$ quelconques, mais non divisibles par $p$, les différences

$$a^{p-1} - 1 \text{ et } b^{p-1} - 1$$

sont divisibles par $p$; donc, si $a - b$ n'est pas divisible par $p$, on a

$$U_{p-1} = \frac{a^{p-1} - b^{p-1}}{a - b} \equiv 0, \text{ (Mod. } p).$$

Par conséquent, les différents termes des séries récurrentes de première espèce contiennent, en exceptant les diviseurs de $Q = ab$ et de $\delta = a - b$, tous les nombres premiers en facteurs.

Mais, s'il est vrai que $p$ divise $U_{p-1}$, on peut, dans la plupart des cas, trouver un terme de rang inférieur à $p - 1$, et divisible par $p$. Désignons par $\omega$ le *rang d'arrivée* ou *d'apparition* du nombre premier $p$ dans la série des $U_n$; il résulte des principes exposés (Section XI), que l'on a, pour $k$ entier et positif,

$$U_{k\omega} \equiv 0, \text{ (Mod. } p);$$

ainsi, tous les termes divisibles par $p$ ont un rang égal à un multiple quelconque du rang d'apparition.

Il résulte encore des principes exposés (Section XIII), que les termes, dont le rang est un multiple quelconque de $(p - 1)\, p^{\lambda - 1}$, sont divisibles par $p^\lambda$; mais il peut exister d'autres termes divisibles par $p^\lambda$, pour deux raisons bien différentes; 1° lorsque le rang d'arrivée $\omega$ de $p$ diffère de $p - 1$; 2° lorsque le nombre premier $p$ arrive pour la première fois à une puissance supérieure à la première; mais, cela connu, il est facile de tenir compte de ces singularités. En général, si $m$ désigne un nombre quelconque premier avec $Q$, et $\phi\,(m)$ *l'indicateur de* $m$, c'est-à-dire le nombre des entiers inférieurs et premiers à $m$, on a la congruence

$$(135) \qquad U_{\phi(m)} \equiv 0, \quad \text{(Mod. } m);$$

cette congruence correspond au *théorème de* FERMAT *généralisé* par EULER. Inversement, si l'on a

$$U_n \equiv 0, \quad \text{(Mod. } m),$$

on en déduit

$$n = k\mu,$$

$\mu$ désignant un certain diviseur de $\phi\,(m)$, et $k$ un entier positif quelconque.

Les résultats que nous venons d'obtenir conduisent à la forme linéaire des diviseurs premiers de $U_n$. En effet, si $\omega$ désigne toujours le rang d'arrivée de $p$, on a, puisque $U_{p-1}$ est divisible par $p$,

$$p - 1 = k_0\omega,$$

et, par suite

$$(136) \qquad p = k_0\omega + 1.$$

Nous appellerons *diviseurs propres* de $U_n$ tous les facteurs premiers de $U_n$ que l'on ne rencontre pas dans les termes de rang inférieur, et *diviseurs impropres*, les facteurs premiers contenus préalablement dans les termes de la série. On a alors les deux propositions suivantes :

THÉORÈME I : *Les diviseurs impropres des termes $U_n$ des fonctions simplement périodiques sont des diviseurs propres des termes dont le rang est un diviseur de n.*

THÉORÈME II : *Les diviseurs propres des termes $U_n$ des fonctions périodiques de première espèce appartiennent à la forme linéaire $kn + 1$.*

Enfin, si l'on observe que l'on a trouvé

$$U_{2n} = U_n V_n,$$

on a encore :

THÉORÈME III : *Les diviseurs propres de $V_n$ appartiennent à la forme linéaire $2kn + 1$.*

On déduit encore de ce qui précéde la démonstration du théorème suivant, qui n'est qu'un cas particulier du théorème de LEJEUNE-DIRICHLET, sur les progressions arithmétiques :

THÉORÈME IV : *Quel que soit l'entier m, il y a une série indéfinie de nombres premiers de la forme linéaire $km + 1$.*

En effet, il est d'abord évident que, pour une valeur suffisamment grande de $n$, le terme $U_n$ posséde nécessairement un ou plusieurs diviseurs propres de la forme $kn + 1$. Par conséquent, si l'on fait successivement $n$ égal à

$$m, \; pm, \; p^2m, \; p^3m, \; \ldots \; p^\lambda m,$$

$p$ étant premier, les termes correspondants possèdent tous, à partir d'un certain rang, des diviseurs de la forme considérée ; le théorème est donc démontré.

Il résulte encore, du théorème I (Section XX), que ces diviseurs appartiennent en outre aux diviseurs de la forme quadratique $x^2 \pm py^2$, suivant que l'on prend pour $p$ un nombre premier de la forme $4q + 3$, ou de la forme $4q + 1$.

Les théorèmes précédents permettent encore de déterminer les diviseurs des fonctions numériques de première espèce ; nous donnerons d'abord les deux exemples suivants dus à EULER.

EXEMPLE I : Soit, dans la série de FERMAT,

$$U_{64} = 2^{64} - 1 = 18446\ 74407\ 37095\ 51615,$$

on a, d'après les formules précédentes,

$$U_{64} = U_1 V_1 V_2 V_4 V_8 V_{16} V_{32} \,;$$

on a immédiatement les décompositions en facteurs premiers

$$U_1 = 1, \quad V_1 = 3, \quad V_2 = 5, \quad V_4 = 17, \quad V_8 = 257, \quad V_{16} = 65537\,;$$

et

$$V_{32} = 42949\,67297\,.$$

Les diviseurs de $V_{32}$ appartiennent à la forme linéaire $64k + 1$; en essayant les diviseurs premiers de cette forme

$$193,\ 257,\ 449,\ 577,\ 641,$$

on trouve

$$V_{32} = 641 \times 67\,00417.\,^*$$

L'essai des diviseurs premiers de même forme

$$641,\ 769,\ 1153,\ 1217,\ 1409,\ 1601,\ 2113,$$

et inférieurs à la racine carrée du second facteur de $V_{32}$, indique presque immédiatement que 67 00417 est un nombre premier.

FERMAT avait annoncé, mais sans dire qu'il en eût la démonstration, dans une lettre du 18 Octobre 1640, que la formule $2^{2^n} + 1$ donnait toujours des nombres premiers. Cette formule se trouve en défaut, d'après la décomposition précédente, due à EULER, pour $n = 5$.

On sait, d'autre part, que GAUSS a démontré que l'on peut diviser la circonférence en $2^{2^n} + 1$ parties égales, lorsque ce nombre est premier, et seulement dans ce cas, par la règle et le compas. Nous indiquerons plus loin une méthode de recherche du mode de composition des nombres de cette forme, basée sur la distribution des nombres premiers dans la série de PELL. Par la méthode que nous venons d'exposer, en supposant que le nombre

$$2^{2^6} + 1 = 18446\,74407\,37095\,51617\,,$$

soit premier, il faudrait à un seul calculateur, pour le démontrer, tout en profitant de la forme $128k + 1$, imposée aux diviseurs de ce nombre, environ *trois mille ans* de travail assidu.† Par notre méthode, il suffit de *trente heures*, pour décider si ce nombre est premier ou composé.

EXEMPLE II: Soit encore, dans la série de FERMAT, le terme

$$U_{31} = 2^{31} - 1 = 21474\,83647$$

dont le rang 31 est un nombre premier. Les diviseurs de $U_{31}$ sont, sans exception, des diviseurs propres appartenant à la forme linéaire $62k + 1$. Mais, d'autre part (Section VIII, Théorème I), en tenant compte des formes quadratiques de ses diviseurs, ou es formes linéaires correspondantes $8k' \pm 1$,

---

* Il est inutile, d'après la loi de répétition, d'essayer 257 qui se trouve dans $V_8$. Nous avons démontré que les diviseurs de $V_{32}$ appartiennent à la forme $128k + 1$. (*Académie de Turin*, janvier 1878)

† *Aux mathématiciens de toutes les parties du monde.—Communication sur la décomposition des nombres en leurs facteurs simples.* Par M. F. LANDRY. Paris, 1867. (Note de la page 8.)

on voit que tout diviseur premier de $U_{31}$ appartient nécessairement à l'une des formes linéaires

$$248k + 1, \quad 248k + 63.$$

"Or, EULER* nous apprend qu'après avoir essayé tous les nombres premiers contenus dans ces deux formes, jusqu'à 46339, racine du nombre $2^{31} - 1$, il n'en a trouvé aucun qui fût diviseur de ce nombre; d'où il faut conclure conformément à une assertion de FERMAT, que le nombre $2^{31} - 1$ est un nombre premier. C'est le plus grand de ceux qui aient été vérifiés jusqu'à présent." (LEGENDRE, Théorie des Nombres, 3e édition, t. I, pag. 229. Paris, 1830.)

EXEMPLE III: On connaissait, depuis quelques années, un nombre premier plus grand que le précédent, indiqué par PLANA, dans son *Mémoire sur la Théorie des Nombres*, du 20 Novembre 1859.† Soit, en effet

$$V_{29} = 3^{29} + 1;$$

ce nombre a tous ses diviseurs propres de la forme $58k + 1$; mais d'autre part, ces diviseurs appartiennent à la forme quadratique $x^2 + 3y^2$, et, par suite, aux formes linéaires $12k + 1$ et $12k + 7$. En combinant l'une de ces formes avec la précédente, on trouve que les diviseurs de $V_{29}$ sont de l'une des deux formes

$$348k + 1, \quad \text{ou} \quad 348k + 175.$$

PLANA a ainsi trouvé la décomposition

$$V_{29} = 2^2 \times 6091 \times 28168\,76431,$$

et vérifié que le dernier facteur est premier. Il a encore indiqué (*loc. cit.*, pag. 140 et 141) que le quotient

$$\frac{3^{29} - 1}{2 \times 59} = 58\,16133\,67499,$$

n'a pas de diviseur premier inférieur à 52259, et que le nombre $2^{53} - 1$ n'a pas de diviseur inférieur à 50033. Ces trois assertions sont inexactes; on a

$$3^{29} - 1 = 2 \times 59 \times 28537 \times 203\,81027,$$
$$3^{29} + 1 = 2^2 \times 523 \times 6091 \times 53\,85997,$$
$$2^{53} - 1 = 6361 \times 69431 \times 203\,94401.$$

Nous ajouterons que l'on trouve encore dans la mémoire de PLANA, la décomposition

$$2^{41} - 1 = 13367 \times 1645\,11353.$$

* *Lettre à Bernoulli*, en 1771,—*Mémoires de l'Académie de Berlin*, année 1772, pag. 36.

† *Memorie della Reale Accademia delle Scienze di Torino*, 2e série, t. XX, p. 139. Turin, 1863.

EXEMPLE IV: Nous donnerons encore quelques exemples de décomposition de la fonction numérique

$$(2m)^{2m} - 1,$$

qui joue un rôle assez important dans les congruences de degré supérieur. Nous avons trouvé les résultats suivants:

$$\left\{\begin{array}{l}
14^7 - 1 = 13 \times 81\,08731, \\
14^7 + 1 = 3 \times 5 \times 70\,27567, \\
20^{10} - 1 = 3 \times 7 \times 11 \times 19 \times 61 \times 251 \times 1\,52381, \\
20^{10} + 1 = 41 \times 401 \times 2801 \times 2\,22361, \\
22^{11} - 1 = 3 \times 7 \times 67 \times 353 \times 11764\,69537, \\
22^{11} + 1 = 23 \times 89 \times 28\,54510\,51007, \\
24^{12} - 1 = 5^2 \times 7 \times 13 \times 23 \times 73 \times 79 \times 349 \times 577 \times 601, \\
24^{12} + 1 = 97 \times 3\,31777 \times 11347\,93633, \\
28^{14} - 1 = 3^3 \times 29 \times 113 \times 13007 \times 35771 \times 44\,22461, \\
30^{15} - 1 = 7^2 \times 19 \times 29 \times 12211 \times 8\,37931 \times 519\,41161, \\
30^{15} + 1 = 11 \times 13 \times 31 \times 67 \times 271 \times 4831 \times 71261 \times 5\,17831,
\end{array}\right.$$

dont nous donnerons plus tard l'application à de nouvelles recherches sur le dernier théorème de FERMAT.

## SECTION XXV.

### *De l'apparition des nombres premiers dans les séries récurrentes de seconde et de troisième espèce.*

En désignant toujours par $p$ un nombre premier quelconque, on sait que le reste de la division de $\Delta^{\frac{p-1}{2}}$ par $p$ est toujours égal à 0, à $+1$, ou à $-1$, suivant que $\Delta$ est un multiple, un résidu quadratique, ou un non-résidu quadratique de $p$. Nous considérerons les cinq cas suivants.

### PREMIER CAS. *$p$ est un diviseur de $P$.*

On a $U_2 = P$, et par conséquent tous les termes $U_n$ de rang pair de la série sont divisibles par $p$; en désignant par $p^\lambda$ la plus haute puissance de $p$ qui divise $P$, les rangs des termes divisibles par $p^{\lambda+\mu}$ seront tous les multiples de $2p^\mu$.

DEUXIÈME CAS. *p est un diviseur de Q.*

Nous avons, par définition,

$$2^n \sqrt{\Delta}\, U_n = (P+\sqrt{\Delta})^n - (P-\sqrt{\Delta})^n,$$
$$2^n V_n = (P+\sqrt{\Delta})^n + (P-\sqrt{\Delta})^n;$$

on a donc, en supprimant les multiples de $Q$, par le remplacement de $\Delta$ par $P^2$, les congruences

$$2^n P U_n \equiv (P+P)^n, \quad (\text{Mod. } Q),$$
$$2^n V_n \equiv (P+P)^n, \quad (\text{Mod. } Q),$$

ou, plus simplement,

(137) $$U_n \equiv P^{n-1}, \quad V_n \equiv P^n, \quad (\text{Mod. } Q).$$

Par conséquent, $U_n$ et $V_n$ ne sont jamais divisibles par $Q$ ou par l'un de ses diviseurs, puisque $P$ et $Q$ ont été supposés premiers entre eux. D'ailleurs ce résultat s'applique aux séries de première et de troisième espèce ; lorsque l'on a $Q = \pm 1$, comme dans les séries de PELL et de FIBONACCI, nous n'aurons pas à tenir compte du théorème précédent.

TROISIÈME CAS. *p est un diviseur de* $\Delta$.

Lorsque $p$ est un nombre premier diviseur de $\Delta$, les formules (4) donnent immédiatement,

(138) $$U_p \equiv 0, \quad V_p \equiv P, \qquad (\text{Mod. } p).$$

et, par suite cette proposition :

THÉORÈME : *Dans la série U de seconde espèce, tout diviseur premier p du déterminant* $\Delta$ *est un diviseur de* $U_p$.

Il résulte d'ailleurs des principes exposés précédemment, qu'un diviseur premier impair $p$ de $\Delta$ arrive pour la première fois, dans $U_p$ et *à la première puissance.*

QUATRIÈME CAS. $\Delta$ *est résidu quadratique de p.*

En changeant, dans la première des formules (4), $p$ en $p-1$, on a

$$2^{p-2} U_{p-1} = \frac{p-1}{1} P^{p-2} + \frac{(p-1)(p-2)(p-3)}{1\,.\,2\,.\,3} P^{p-4}\Delta + \ldots + \frac{p-1}{1} P\Delta^{\frac{p-3}{2}};$$

et, en appliquant les résultats obtenus (Section XXI) pour les congruences du triangle arithmétique, on a

$$2^{p-2} U_{p-1} \equiv -\left[P^{p-2} + P^{p-4}\Delta + P^{p-6}\Delta^2 + \ldots + P\Delta^{\frac{p-3}{2}}\right], \quad (\text{Mod. } p),$$

et, par suite

$$2^{p-2} U_{p-1} \equiv - P \frac{P^{p-1} - \Delta^{\frac{p-1}{2}}}{P^2 - \Delta}, \quad (\text{Mod.}\ p)\ .$$

Mais on a, par le théorème de FERMAT, $P^{p-1} \equiv 1$, (Mod. $p$), et, puisque $\Delta$ est résidu quadratique de $p$, il en résulte que $U_{p-1}$ est divisible par $p$. On a donc cette proposition, qui s'applique aux séries de troisième espèce, en tenant compte du signe de $\Delta$:

THÉORÈME: *Dans la série récurrente $U$ de seconde ou de troisième espèce, tout nombre premier $p$, qui admet $\Delta$ pour résidu quadratique, divise le terme $U_{p-1}$.*

La seconde des formules (4) donne

$$2^{p-2} V_{p-1} = P^{p-1} + \frac{(p-1)(p-2)}{1.2} P^{p-3}\Delta + \ldots\ldots + \Delta^{\frac{p-1}{2}},$$

et, par suite

$$2^{p-2} V_{p-1} \equiv P^{p-1} + P^{p-3}\Delta + \ldots\ldots + \Delta^{\frac{p-1}{2}}, \quad (\text{Mod.}\ p),$$

ou bien

$$2^{p-2} V_{p-1} \equiv \frac{P^{p+1} - \Delta^{\frac{p+1}{2}}}{P^2 - \Delta}, \quad (\text{Mod.}\ p)\ .$$

Mais on a, dans le cas présent

$$P^{p+1} \equiv P^2 \quad \text{et} \quad \Delta^{\frac{p+1}{2}} \equiv \Delta, \quad (\text{Mod.}\ p);$$

donc

$$2^{p-2} V_{p-1} \equiv 1, \quad (\text{Mod.}\ p),$$

et finalement, en multipliant par 2 et appliquant le théorème de FERMAT:

(139) $$V_{p-1} \equiv 2, \quad (\text{Mod.}\ p)\ .$$

CINQUIÈME CAS. $\Delta$ *est non-résidu quadratique de $p$.*

On a, comme précédemment,

$$2^p U_{p+1} = \frac{p+1}{1} P^p + \frac{(p+1)p(p-1)}{1.2.3} P^{p-2}\Delta + \ldots\ldots + \frac{p+1}{1} P\Delta^{\frac{p-1}{2}},$$

$$2^p V_{p+1} = P^{p+1} + \frac{(p+1)p}{1.2} P^{p-1}\Delta + \ldots\ldots + \Delta^{\frac{p+1}{2}},$$

et, puisque $p$ est premier,

$$2 U_{p+1} \equiv P\,(1 + \Delta^{\frac{p-1}{2}}),$$

$$2 V_{p+1} \equiv P^2 + \Delta\,.\,\Delta^{\frac{p-1}{2}}\ .$$

Mais, par hypothèse $\Delta$ est non-résidu quadratique de $p$, et, par suite

$$\Delta^{\frac{p-1}{2}} \equiv -1, \quad (\text{Mod.}\ p);$$

on a donc

(140) $$U_{p+1} \equiv 0\,, \quad V_{p+1} \equiv 2Q\,, \quad (\text{Mod. } p)\,;$$

de là, cette proposition :

THÉORÈME : *Dans les séries récurrentes $U_n$ de seconde et de troisième espèce, tout nombre premier $p$, dont $\Delta$ est un non-résidu quadratique, divise $U_{p+1}$.*

Désignons encore par $\omega$ le rang d'arrivée du nombre premier $p$ dans la série des $U_n$, et par $k$ un nombre entier quelconque ; on a

$$U_{k\omega} \equiv 0\,, \quad (\text{Mod. } p)\,;$$

par conséquent, si $p$ n'est pas diviseur de $Q$ ou de $\Delta$, on a

$$k_0\omega = p \mp 1\,,$$

en prenant le signe — ou le signe + suivant que $\Delta$ est résidu ou non-résidu de $p$ ; on en déduit

$$p = k_0\omega \pm 1\,,$$

et, par conséquent :

THÉORÈME : *Dans les séries récurrentes de seconde espèce, les diviseurs propres de $U_\omega$ sont de la forme linéaire $p = k\omega \pm 1$, suivant que $\Delta$ est résidu ou non-résidu de $p$.*

En suivant une marche analogue à celle que nous avons suivie dans le paragraphe précédent, on obtient par la considération des diviseurs de $U_p\lambda$, le théorème suivant.

THÉORÈME : *Il y a une série indéfinie de diviseurs premiers communs aux formes quadratiques $x^2 - Qy^2$ et $x_1^2 - py_1^2$, lorsque $p$ désigne un nombre premier de la forme $4q + 1$ ; et une série indéfinie de diviseurs communs aux deux formes $x^2 - Qy^2$ et $\Delta x_1^2 + py_1^2$, lorsque $p$ désigne un nombre premier de la forme $4q + 3$.*

Nous appliquerons les résultats qui précédent, aux séries de FIBONACCI et de PELL. Pour la première, on a $P = 1$, $Q = -1$, et $\Delta = 5$, d'autre part, on sait,* que le nombre 5 est résidu de tous les nombres premiers qui sont résidus de 5, et non-résidus de tous les nombres premiers impairs qui sont non-résidus de 5 lui-même. Par conséquent :

*Dans la série de* FIBONACCI, *tout nombre $p$ premier impair, de la forme $10q \pm 1$, divise le terme de rang $p - 1$, et tout nombre $p$ premier impair de la forme $10q \pm 3$ divise le terme de rang $p + 1$.*

D'ailleurs, les nombres 2 et 5 divisent respectivement les termes dont le rang est un multiple de 3 ou de 5.

---

* GAUSS.—*Disquisitiones Arithmeticæ.* Nos. 121, 122 et 123.

Pour la série de PELL, $P = 2$, $Q = -1$, $\Delta = 2^2 \times 2$; d'autre part, on sait que le nombre 2 est résidu de tout nombre qui n'est pas divisible par 4, ni par aucun nombre premier de la forme $8q + 3$ ou $8q + 5$, et non-résidu de tous les autres; par conséquent:

*Dans la série de* PELL, *tout nombre premier $p$ de la forme $8q \pm 1$ divise $U_{p-1}$, et tout nombre premier $p$ de la forme $8q \pm 3$ divise $U_{p+1}$.*

Les théorèmes que nous venons de démontrer conduisent à la décomposition des termes des séries récurrentes de seconde et de troisième espèce, en facteurs premiers. On a ainsi, par exemple, dans la série de FIBONACCI:

$$U_{41} = 1655\ 80141 = 2789 \times 59369,$$
$$U_{53} = 5\ 33162\ 91173 = 953 \times 559\ 45741,$$
$$U_{59} = 95\ 67220\ 26041 = 353 \times 27102\ 60697.$$

Nous ajouterons une remarque importante dont on retrouve l'origine dans la correspondance de FERMAT, mais seulement pour les séries de première espèce.

Soit encore, par exemple, la série de FIBONACCI; les nombres premiers $p$, des formes linéaires $20q + 13$ et $20q + 17$, divisent $U_{p+1}$, et l'on a

$$p + 1 = 20q + 14 \text{ ou } p + 1 = 20q + 18,$$

et aussi

$$U_{20q+14} = U_{10q+7} V_{10q+7}, \text{ et } U_{20q+18} = U_{10q+9} V_{10q+9};$$

mais, d'autre part, les diviseurs de $V_{2n+1}$ appartiennent aux formes linéaires $20q + 1, 9, 11, 19$; par conséquent, les nombres premiers de la forme $20q + 13$ ou $20q + 17$ divisent respectivement $U_{10q+7}$ et $U_{10q+9}$, et disparaissent de la série des $V_n$ qui ne contient donc pas tous les nombres premiers. En appliquant ce raisonnement aux séries de FERMAT et de PELL, on en déduit les principes suivants:

*Dans la série de* FIBONACCI, *les termes $V_n$ ne contiennent aucun nombre premier des formes linéaires $20q + 13$, $20q + 17$.*

*Dans la série de* FERMAT, *les termes $V_n$ ne contiennent aucun nombre premier de la forme $8q + 7$.*

*Dans la série de* PELL, *les termes $V_n$ ne contiennent aucun nombre premier de la forme $8q + 5$.*

Nous donnons dans le tableau de la page 299, la décomposition en facteurs premiers des termes de la série de FIBONACCI, limitée aux soixante premiers termes.

## TABLEAU DES FACTEURS PREMIERS DE LA SÉRIE RÉCURRENTE DE LÉONARD DE PISE.

| $n$. | $u_n$. | Div. impropres. | Div. propres. | $n$. | $u_n$. | Diviseurs impropres. | Diviseurs propres. |
|---|---|---|---|---|---|---|---|
| 1 | 1 | — | 1. | 31 | 13 46269 | — | 557 × 2417. |
| 2 | 1 | — | 1. | 32 | 21 78309 | 3 × 7 × 47. | 2207. |
| 3 | 2 | — | 2. | 33 | 35 24578 | 2 × 89. | 19801. |
| 4 | 3 | — | 3. | 34 | 57 02887 | 1597. | 3571. |
| 5 | 5 | — | 5. | 35 | 92 27465 | 5 × 13. | 1 41961. |
| 6 | 8 | $2^3$. | — | 36 | 149 30352 | $2^4 \times 3^3 \times 17 \times 19$. | 107. |
| 7 | 13 | — | 13. | 37 | 211 57817 | — | 73 × 149 × 2221. |
| 8 | 21 | 3. | 7. | 38 | 390 88169 | 37 × 113. | 9349. |
| 9 | 34 | 2. | 17. | 39 | 632 45986 | 2 × 233. | 1 35721. |
| 10 | 55 | 5. | 11. | 40 | 1023 34155 | 3 × 5 × 7 × 11 × 41. | 2161. |
| 11 | 89 | — | 89. | 41 | 1655 80141 | — | 2789 × 59369. |
| 12 | 144 | $2^4 \times 3^2$. | — | 42 | 2679 14296 | $2^3 \times 13 \times 29 \times 421$. | 211. |
| 13 | 233 | — | 233. | 43 | 4334 94437 | — | 4334 94437. |
| 14 | 377 | 13. | 29. | 44 | 7014 08733 | 3 × 89 × 199. | 43 × 307. |
| 15 | 610 | 2 × 5. | 61. | 45 | 11349 03170 | 2 × 5 × 17 × 61. | 1 09441. |
| 16 | 987 | 3 × 7. | 47. | 46 | 18363 11903 | 28657. | 139 × 461. |
| 17 | 1597 | — | 1597. | 47 | 29712 15073 | — | 29712 15073. |
| 18 | 2584 | $2^3 \times 17$. | 19. | 48 | 48075 26976 | $2^6 \times 3^2 \times 7 \times 23 \times 47$. | 1103. |
| 19 | 4181 | — | 37 × 113 | 49 | 77787 42049 | 13. | 97 × 61 68709. |
| 20 | 6765 | 3 × 5 × 11. | 41. | 50 | 1 25862 69025 | $5^2 \times 11 \times 3001$. | 101 × 151. |
| 21 | 10946 | 2 × 13 | 421. | 51 | 2 03650 11074 | 2 × 1597. | 63 76021. |
| 22 | 17711 | 89. | 199. | 52 | 3 29512 80099 | 3 × 233 × 521. | 90481. |
| 23 | 28657 | — | 28657. | 53 | 5 33162 91173 | — | 953 × 559 45741. |
| 24 | 46368 | $2^4 \times 3^2 \times 7$. | 23. | 54 | 8 62675 71272 | $2^3 \times 17 \times 19 \times 53 \times 109$. | 5779. |
| 25 | 75025 | $5^2$. | 3001. | 55 | 13 95838 62445 | 5 × 89. | 661 × 4 74541 |
| 26 | 1 21393 | 233. | 521. | 56 | 22 58514 33717 | $3 \times 7^2 \times 13 \times 29 \times 281$. | 14503. |
| 27 | 1 96418 | 2 × 17. | 53 × 109. | 57 | 36 54352 96162 | 2 × 37 × 113. | 43 71901. |
| 28 | 3 17811 | 3 × 13 × 29. | 281. | 58 | 59 12867 29879 | 5 14229. | 59 × 19489. |
| 29 | 5 14229 | — | 5 14229. | 59 | 95 67220 26041 | — | 353 × 27102 60697. |
| 30 | 8 32040 | $2^3 \times 5 \times 11 \times 61$. | 31. | 60 | 154 80087 55920 | $2^4 \times 3^2 \times 5 \times 11 \times 31 \times 41 \times 61$. | 2521. |

## SECTION XXVI.

### *Sur la périodicité des fonctions numériques et sur la géneralisation du* CANON ARITHMETICUS.

Les résultats développés dans les deux sections précédentes, conduisent immédiatement à la périodicité numérique des fonctions que nous étudions ici, par la considération de leurs résidus suivant un module premier $p$ ou suivant un module quelconque $m$. Cette question a été présentée sous une forme différente, et seulement pour les séries de première espèce, par GAUSS, dans les *Disquisitiones Arithmeticæ*, sous le nom de *théorie des indices*, et développée par JACOBI dans le *Canon Arithmeticus*. Tous ces résultats peuvent être résumés et généralisés, dans le théorème fondamental suivant, qui contient une extension du *Théorème de* FERMAT *généralisé* par EULER.

THÉORÈME FONDAMENTAL: *Si l'on désigne par m un nomber premier avec le produit des racines d'une équation du second degré à coefficients commensurables,*

$$m = p^{\pi} r^{\rho} s^{\sigma} \ldots ,$$

*par $\Delta$ le discriminant de l'équation, et par $\left(\frac{\Delta}{p}\right)$ le reste de la division de $\Delta^{\frac{p-1}{2}}$ par $p$, et égal à $+1$ ou à $-1$, suivant que $\Delta$ est résidu quadratique, ou non-résidu quadratique de $p$; et, soit, de plus*

$$\Psi(m) = p^{\pi-1} r^{\rho-1} s^{\sigma-1} \ldots \left[p - \left(\frac{\Delta}{p}\right)\right]\left[r - \left(\frac{\Delta}{r}\right)\right]\left[s - \left(\frac{\Delta}{s}\right)\right] \ldots ,$$

*on a la congruence*

(142) $$U_{\psi(m)} \equiv 0, \quad (\text{Mod. } m).$$

*Réciproquement, si $U_n$ est divisible par m, le nombre n est un multiple quelconque d'un certain diviseur $\mu$ de $\Psi(m)$.*

Ce nombre $\mu$ est, par extension, l'exposant auquel appartient $a$ ou $b$ par rapport au module $m$; on retrouve le théorème d'EULER, en supposant $b = 1$.

Quant à la périodicité numérique des résidus, elle résulte des formules d'addition. On a d'abord, en faisant $n = k\omega$ dans les formules (49),

$$2U_{m+k\omega} = U_m V_{k\omega} + U_{k\omega} V_m,$$
$$2V_{m+k\omega} = V_m V_{k\omega} + \Delta U_m U_{k\omega};$$

par conséquent, si $\omega$ désigne le rang d'arrivée du nombre premier $p$ dans la série des $U_n$, on a

(143) $$\left.\begin{aligned} 2U_{m+k\omega} &\equiv V_{k\omega} U_m, \\ 2V_{m+k\omega} &\equiv V_{k\omega} V_m, \end{aligned}\right\} (\text{Mod. } p).$$

Supposons d'abord qu'il s'agisse des fonctions de première espèce, ou lorsque $\Delta$ est résidu de $p$, des fonctions de deuxième et de troisième espèce; déterminons le nombre $k$ de telle sorte que l'on ait

$$V_{k\omega} \equiv 2, \quad (\text{Mod. } p),$$

ce qui a lieu pour $k\omega = p - 1$, mais aussi, dans la plupart des cas, pour un certain diviseur $\pi$ de $p - 1$; on aura alors, pour $h$ entier et positif, mais quelconque, les formules

$$(144) \qquad \left.\begin{aligned} U_{m+h\pi} &\equiv U_m, \\ V_{m+h\pi} &\equiv V_m, \end{aligned}\right\} \quad (\text{Mod. } p).$$

Celles ci sont analogues aux formules qui donnent la périodicité des fonctions circulaires; leur application conduit, lorsque l'on remplace le nombre premier $p$ par un module quelconque $m$, et que l'on tient compte de la *loi de répétition*, à des formules nouvelles contenant la généralisation de résultats indiqués par ARNDT et SANCERY.*

Mais dans le cas des séries de seconde et de troisième espèce il n'en est plus absolument de même, lorsque $\Delta$ est non-résidu de $p$. En posant $\omega' = p + 1$, on a alors;

$$\left.\begin{aligned} U_{m+\omega'} &\equiv Q\,U_m, \\ V_{m+\omega'} &\equiv Q\,V_m, \end{aligned}\right\} \quad (\text{Mod. } p),$$

et, plus généralement, pour $k$ entier et positif,

$$(145) \qquad \left.\begin{aligned} U_{m+k\omega'} &\equiv Q^k U_m, \\ V_{m+k\omega'} &\equiv Q^k V_m, \end{aligned}\right\} \quad (\text{Mod. } p);$$

par conséquent, si $\mu$ désigne l'exposant auquel appartient $Q$ suivant le module $p$, on aura

$$\left.\begin{aligned} U_{m+k\mu\omega'} &\equiv U_m, \\ V_{m+k\mu\omega'} &\equiv V_m, \end{aligned}\right\} \quad (\text{Mod. } p).$$

Ainsi dans ce dernier cas, l'amplitude de la période est égale à $\mu\omega'$.

## SECTION XXVII.

### *Sur l'inversion du théorème de* FERMAT *et sur la vérification des grands nombres premiers.*

On sait que le théorème de WILSON qui consiste, pour $p$ premier, dans la congruence

$$1.2.3\ldots\ldots(p-1) \equiv -1, \quad (\text{Mod. } p),$$

* *Journal de Crelle*, t. XXXI; pag. 260 et suiv. 1846.—*Bulletin de la Société Mathématique de France*, t. IV. pag. 17 et suiv. Paris, 1876.

s'applique exclusivement aux nombres premiers, et donne, par suite, un procédé théorique, mais illusoire dans la pratique, pour reconnaître si un nombre donné est premier. Il n'en est pas de même du théorème de FERMAT. En désignant par $a$ un nombre inférieur à $p$, on a

$$a^{p-1} \equiv 1, \quad (\text{Mod. } p);$$

mais ce théorème n'est pas restreint aux nombres premiers, et cette congruence peut être vérifiée pour des modules composés ; ainsi, on a, par exemple,

$$2^{37 \times 73 - 1} \equiv 1, \quad (\text{Mod. } 37 \times 73).$$

Cependant, on peut énoncer le théorème suivant que l'on doit considérer comme la proposition réciproque de celle de FERMAT.

THÉORÈME: *Si $a^x - 1$ est divisible par $p$, lorsque $x = p - 1$, et n'est pas divisible par $p$, pour $x$ inférieur à $p - 1$, le nombre $p$ est premier.*

On sait que, dans ce cas, $a$ est une *racine primitive de $p$*; de plus, il est facile de voir que si $p - 1$ est égal à une puissance de puissance de 2, $a$ est non-résidu quadratique de $p$. Ce théorème rentre dans le suivant, dont la démonstration résulte immédiatement des propriétés des fonctions numériques simplement périodiques, et s'applique aux trois espèces de séries:

THÉORÈME FONDAMENTAL: *Si dans l'une des séries récurrentes $U_n$, le terme $U_{p-1}$ est divisible par $p$, sans qu'aucun des termes de la série dont le rang est un diviseur de $p - 1$ le soit, le nombre $p$ est premier; de même si $U_{p+1}$ est divisible par $p$, sans qu'aucun des termes de la série dont le rang est un diviseur de $p + 1$ le soit, le nombre $p$ est premier.*

En effet, puisque $p$ divise $U_{p\pm 1}$, tous les termes divisibles par $p$ ont un rang égal à un multiple quelconque d'un certain diviseur de $p \pm 1$; d'autre part, supposons $p$ non premier et égal, par exemple, au produit de deux nombres premiers $r$ et $s$, on a

$$U_{r\pm 1} \equiv 0, \quad (\text{Mod. } r), \qquad U_{s\pm 1} \equiv 0, \quad (\text{Mod. } s),$$

et, par suite le terme dont le rang est $(r \pm 1)(s \pm 1)$ est divisible par $rs$; mais, par hypothèse $p$ divise le terme de rang $rs \pm 1$, et, par conésquent aussi, le terme dont le rang est égal à la différence des précédents, c'est-à-dire

$$(r \pm 1)(s \pm 1) - (rs \pm 1),$$

ou bien

$$\pm r \pm s \pm 1 \pm 1.$$

Mais ce dernier nombre est évidemment plus petit que $rs$; par conséquent, si $p$ n'est pas premier, il divise un terme dont le rang est inférieur à $p \pm 1$; c'est ce que ne suppose pas l'énoncé.

On obtiendrait le même résultat en supposant $p$ égal à un nombre impair quelconque, en faisant voir (Section XXVI, Théor. fond.) que

$$m \pm 1 - \psi(m)$$

est plus petit que $m \pm 1$.

Dans l'application de ce théorème, on calcule les termes dont le rang est un diviseur quelconque de $p \pm 1$, au moyen des formules d'addition et de multiplication des fonctions numériques, que nous avons exposées ci-dessus. Nous donnerons d'abord un exemple numérique très-simple.

EXEMPLE: Soit

$$2^7 - 1 = 127.$$

Pour savoir si 127 est premier, nous calculons $U_{128}$ dans la série de FIBONACCI; on a alors les formules

$$V_{4n+2} = V_{2n+1}^2 + 2, \qquad V_{4n} = V_{2n}^2 - 2;$$

on forme ainsi le tableau

$$\begin{aligned} U_4 &= U_2\,(V_1^2 + 2) = U_2 \times 3, \\ U_8 &= U_4\,(V_2^2 - 2) = U_4 \times 7, \\ U_{16} &= U_8\,(V_4^2 - 2) = U_8 \times 47, \\ U_{32} &= U_{16}\,(V_8^2 - 2) = U_{16} \times 2207, \\ U_{64} &= U_{32}\,(V_{16}^2 - 2) = U_{32} \times 48\,70847, \\ U_{128} &= U_{64}\,(V_{32}^2 - 2) = U_{64} \times 2732\,51504\,97407. \end{aligned}$$

Or 127 divise le dernier facteur et ne divise aucun des précédents, ainsi $2732\,51504\,97407 = 127 \times 18\,68122\,08641$, par conséquent 127 est un nombre premier. On simplifie considérablement le calcul par la méthode des congruences, en remplaçant continuellement les nombres $V_2$, $V_4$, $V_8$, .... par leurs résidus suivant le module 127. En tenant compte de cette observation, le tableau précédent devient:

$$\left.\begin{aligned} V_4 &= 3^2 - 2 = 7, \\ V_8 &= 7^2 - 2 = 47, \\ V_{16} &= 47^2 - 2 \equiv 48, \\ V_{32} &\equiv 48^2 - 2 \equiv 16, \\ V_{64} &\equiv 16^2 - 2 \equiv 0. \end{aligned}\right\} \quad (\text{Mod. } 127).$$

Cette méthode de vérification des grands nombres premiers, qui repose sur le principe que nous venons de démontrer, est la *seule méthode directe et pratique*, connue actuellement, pour résoudre le problème en question; elle est opposée, pour ainsi dire, à la méthode de vérification d'EULER, déduite de la consi-

dération des résidus potentiels. Dans celle-ci, on divise le nombre soupçonné premier, par des nombres inférieurs à sa racine carrée, et qui appartiennent à des formes linéaires déterminées que l'on doit d'abord calculer; *le dividende est constant, et le diviseur variable,* mais inférieur, il est vrai, au nombre essayé; c'est *l'insuccès* de ces divisions dont le nombre est considérable, malgré la forme linéaire du diviseur, qui conduit à affirmer que le nombre essayé est premier. Dans notre méthode, au contraire, on divise, par le nombre soupçonné premier, des nombres d'un calcul facile, obtenus par la multiplication des fonctions numériques; ici le *dividende est variable et le diviseur constant;* par conséquent, on remplace les divisions par de simples soustractions, si l'on a calculé préalablement les dix premiers multiples de ce diviseur constant; en outre, le nombre des opérations est peu considérable; c'est le *succès* de l'opération qui conduit à affirmer que le nombre essayé est premier. Ainsi, en cas de réussite, notre méthode est affranchie de l'incertitude des calculs numériques.

Pour vérifier la dernière assertion du P. MERSENNE, sur le nombre supposé premier

$$2^{257} - 1,$$

et qui a *soixante-dix-huit* chiffres, il faudrait à l'humanité tout entière, formée de mille millions d'individus, calculant simultanément et sans interruption, un temps supérieur à un nombre de siècles representé par un nombre de vingt chiffres; par notre méthode, il suffit d'effectuer successivement les carrés de 250 nombres ayant 78 chiffres, au plus; cette opération ne demanderait pas, à deux calculateurs habiles contrôlant leurs opérations, plus de huit mois de travail. Nous appliquerons d'abord le théorème fondamental à la vérification des grands nombres premiers de la série de FERMAT qui appartiennent à la forme

$$p = 2^{4q+3} - 1,$$

dans laquelle nous supposerons l'exposant $4q + 3$ égal à un nombre premier tel que $8q + 7$ soit un nombre composé. En effet, si $4q + 3$ n'est pas premier, le nombre $p$ est composé; d'autre part, nous avons démontré (Section XXIII) que si $4q + 3$ et $8q + 7$ sont premiers, le nombre $p$ est encore composé.

En supposant $p$ premier, on a immédiatement

$$A \equiv 2^3 - 1, \quad (\text{Mod. } 5);$$

donc, dans cette hypothèse $p$ est non-résidu de 5, et divise le terme dont rang est égal à $p + 1$ ou à l'un des diviseurs de $p + 1$, dans la série de

FIBONACCI; mais tous ces diviseurs sont de la forme $2^\lambda$, et pour former les termes qui correspondent à ces rangs, il suffit d'appliquer les formules de duplication des fonctions numériques. On a alors

$$U_{2^{\lambda+1}} = U_{2^\lambda} V_{2^\lambda} \quad \text{et} \quad V_{2^{\lambda+1}} = [V_{2^\lambda}]^2 - 2(-1)^{2^\lambda},$$

et l'application du théorème fondamental donne le principe suivant:

THÉORÈME II: *Soit le nombre* $p = 2^{4q+3} - 1$ *pour lequel* $4q + 3$ *est premier, et* $8q + 7$ *composé; on forme la série* $r_n$

$$1,\ 3,\ 7,\ 47,\ 2207,\ \ldots\ldots$$

*par la relation, pour* $n > 1$,

$$r_{n+1} = r_n^2 - 2;$$

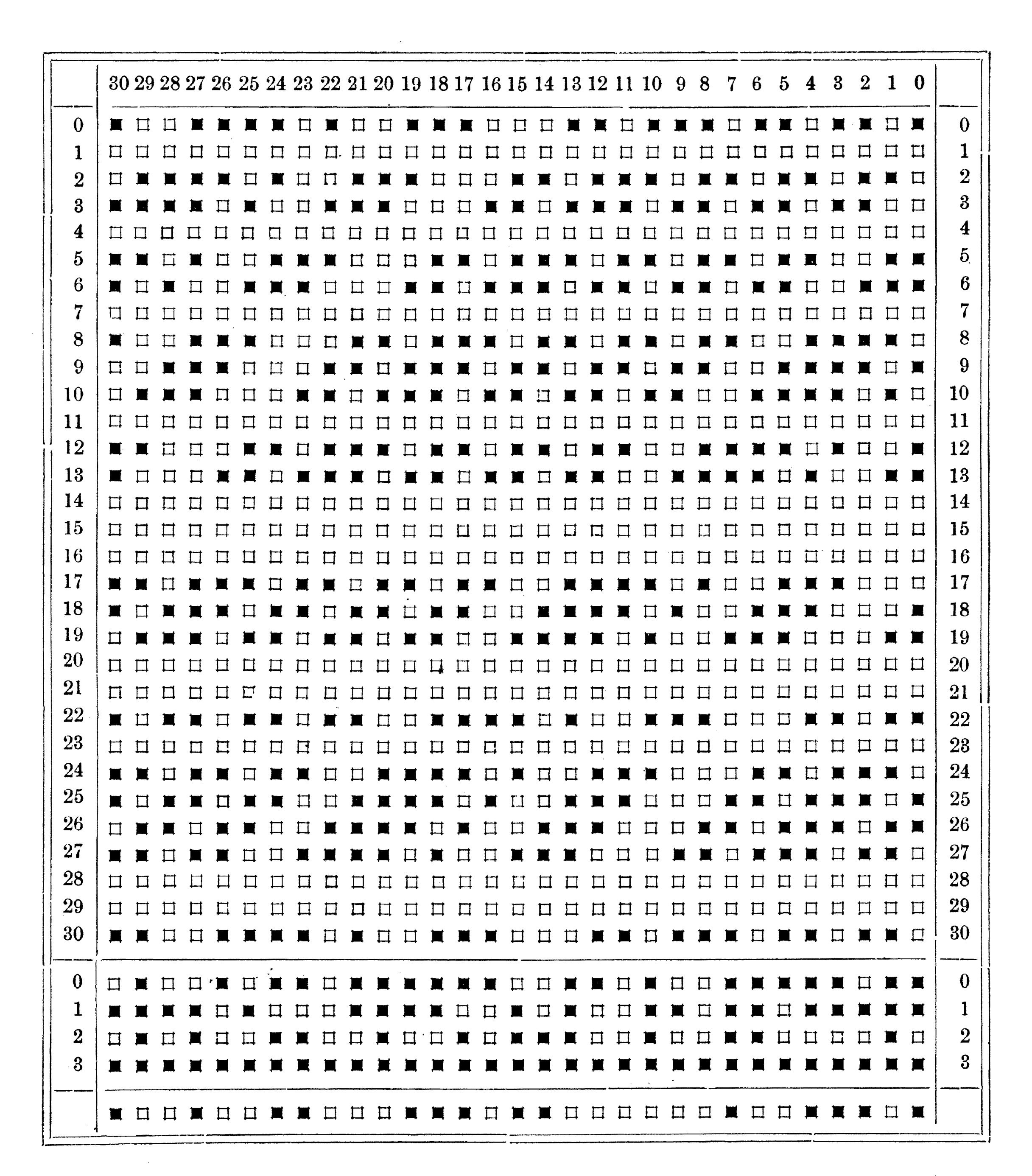
*le nombre* $p$ *est premier lorsque le rang du premier terme, divisible par* $p$, *occupe un rang compris entre* $2q + 1$ *et* $4q + 2$; *le nombre* $p$ *est composé, si aucun des* $4q + 2$ *premiers termes de la série n'est divisible par* $p$; *enfin, si* $\alpha$ *désigne le rang du premier terme divisible par* $p$, *les diviseurs de* $p$ *appartiennent à la forme linéaire* $2^\alpha K \pm 1$, *combinée avec celles des diviseurs de* $x^2 - 2y^2$.

Dans la pratique, on calcule par congruences, en ne conservant que les résidus suivant le module $p$, ainsi que nous l'avons montré précédemment pour le nombre $p = 2^7 - 1$. Nous avons indiqué un autre procédé de calcul, qui repose sur l'emploi du système de numération binaire, et qui conduit à la construction d'un mécanisme propre à la vérification des grands nombres premiers.

Dans ce système de numération, la multiplication consiste simplement dans le déplacement longitudinal du multiplicande; d'autre part, il est clair que le reste de la division de $2^m$ par $2^n - 1$ est égal à $2^r$, $r$ désignant le resté de la division de $m$ par $n$; par conséquent dans l'essai de $2^{31} - 1$, par exemple, il suffira d'opérer sur des nombres ayant, au plus, 31 chiffres. Le tableau de la page 306 donne le calcul du résidu de $V_{2^{26}}$ déduit du résidu de $V_{2^{25}}$ suivant le module $2^{31} - 1$, par la formule

$$V_{2^{26}} \equiv (V_{2^{25}})^2 - 2, \quad (\text{Mod. } 2^{31} - 1);$$

les carrés noirs représentent les unités des différents ordres du système binaire, et les carrés blancs représentent les zéros. La première ligne est le résidu de $V_{2^{25}}$; les 31 premières lignes numérotées 0 — 30 figurent le carré de $V_{2^{25}}$; les 4 lignes numérotées 0, 1, 2, 3 du bas de la page indiquent l'addition des unités de chaque colonne, avec les reports; on a retranché une unité de la première colonne à gauche; enfin la dernière ligne est le résidu de $V_{2^{26}}$.



CALCUL DU RÉSIDU DE $V_{2^{26}}$ AU MOYEN DE $V_{2^{25}}$ SUIVANT LE MODULE $2^{31} - 1$.

Le tableau de la page 307 contient l'ensemble de tous les résidus de $V_2$, $V_{2^2}$, $V_{2^3}$, .... $V_{2^{29}}$, $V_{2^{30}}$ suivant le module $2^{31} - 1$. La dernière ligne, entièrement composée de zéros, nous montre que $2^{31} - 1$ est premier.

| | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | 0 |
| 1 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | 1 |
| 2 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | ■ | 2 |
| 3 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | 3 |
| 4 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | □ | □ | □ | ■ | □ | □ | ■ | ■ | ■ | ■ | ■ | 4 |
| 5 | □ | □ | □ | □ | □ | □ | □ | □ | ■ | □ | □ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | □ | ■ | ■ | ■ | ■ | ■ | ■ | 5 |
| 6 | ■ | ■ | ■ | □ | □ | □ | ■ | □ | □ | ■ | □ | ■ | □ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | □ | ■ | ■ | □ | ■ | □ | □ | ■ | ■ | □ | 6 |
| 7 | □ | ■ | ■ | □ | ■ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | ■ | □ | □ | □ | □ | ■ | □ | ■ | ■ | ■ | □ | □ | 7 |
| 8 | □ | □ | ■ | □ | ■ | □ | □ | □ | ■ | □ | ■ | □ | □ | ■ | □ | □ | □ | □ | □ | ■ | ■ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | □ | 8 |
| 9 | □ | □ | □ | □ | ■ | ■ | ■ | □ | □ | □ | □ | □ | ■ | □ | ■ | ■ | □ | ■ | □ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | 9 |
| 10 | □ | □ | ■ | □ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | □ | ■ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | □ | □ | □ | ■ | ■ | □ | ■ | 10 |
| 11 | ■ | ■ | □ | □ | □ | □ | □ | □ | ■ | □ | ■ | ■ | ■ | □ | □ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | □ | □ | □ | □ | ■ | ■ | 11 |
| 12 | □ | ■ | □ | □ | ■ | □ | ■ | □ | ■ | ■ | ■ | □ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | ■ | □ | □ | ■ | ■ | ■ | □ | □ | □ | 12 |
| 13 | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | ■ | □ | ■ | ■ | ■ | □ | ■ | □ | ■ | 13 |
| 14 | ■ | □ | □ | □ | □ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | □ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | ■ | ■ | □ | □ | □ | 14 |
| 15 | □ | ■ | ■ | □ | ■ | □ | ■ | □ | ■ | ■ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | 15 |
| 16 | □ | ■ | □ | ■ | □ | ■ | ■ | ■ | □ | □ | □ | ■ | ■ | □ | □ | ■ | ■ | □ | □ | □ | □ | ■ | ■ | ■ | □ | □ | ■ | ■ | □ | ■ | ■ | 16 |
| 17 | □ | ■ | □ | □ | ■ | ■ | ■ | ■ | ■ | □ | □ | ■ | ■ | ■ | □ | ■ | □ | ■ | □ | ■ | ■ | ■ | □ | □ | □ | □ | ■ | □ | □ | □ | □ | 17 |
| 18 | □ | □ | □ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | □ | ■ | ■ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | □ | □ | ■ | □ | □ | ■ | 18 |
| 19 | □ | □ | □ | ■ | □ | □ | ■ | □ | ■ | □ | □ | ■ | ■ | ■ | □ | ■ | ■ | □ | □ | □ | ■ | □ | □ | □ | □ | □ | □ | ■ | ■ | ■ | ■ | 19 |
| 20 | □ | □ | ■ | ■ | ■ | □ | ■ | ■ | ■ | ■ | ■ | ■ | □ | □ | □ | □ | □ | ■ | ■ | ■ | ■ | □ | □ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | 20 |
| 21 | ■ | ■ | □ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | □ | ■ | □ | □ | ■ | ■ | □ | ■ | □ | □ | ■ | □ | □ | □ | ■ | □ | ■ | □ | □ | 21 |
| 22 | ■ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | ■ | □ | ■ | ■ | ■ | □ | □ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | □ | 22 |
| 23 | □ | ■ | □ | □ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | □ | ■ | ■ | □ | ■ | ■ | ■ | ■ | □ | □ | □ | ■ | ■ | ■ | □ | □ | □ | □ | ■ | 23 |
| 24 | ■ | □ | □ | □ | ■ | ■ | □ | ■ | ■ | ■ | □ | □ | □ | ■ | □ | □ | ■ | ■ | □ | ■ | □ | □ | ■ | □ | □ | ■ | □ | □ | ■ | ■ | ■ | 24 |
| 25 | ■ | □ | □ | ■ | ■ | ■ | ■ | □ | ■ | □ | □ | ■ | ■ | ■ | □ | □ | □ | ■ | ■ | □ | ■ | ■ | ■ | □ | ■ | ■ | □ | ■ | ■ | □ | ■ | 25 |
| 26 | ■ | □ | □ | ■ | □ | □ | ■ | ■ | □ | □ | □ | ■ | ■ | ■ | □ | ■ | ■ | □ | □ | □ | □ | □ | □ | ■ | □ | □ | ■ | ■ | ■ | □ | ■ | 26 |
| 27 | ■ | ■ | ■ | □ | □ | ■ | ■ | □ | ■ | □ | ■ | ■ | ■ | □ | ■ | □ | ■ | □ | ■ | □ | □ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | □ | 27 |
| 28 | ■ | □ | □ | □ | ■ | ■ | □ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | ■ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | □ | □ | □ | ■ | □ | □ | 28 |
| 29 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | 29 |
| 30 | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | 30 |
| | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |

DIAGRAMME DU NOMBRE PREMIER $2^{31} - 1$.

Ce tableau est, en quelque sorte, un fragment du *Canon Arithmeticus*, correspondant au nombre premier $2^{31} - 1$ pour la racine primitive $\dfrac{1 \pm \sqrt{5}}{2}$.

On pourrait ainsi construire les *diagrammes* des nombres premiers de la forme $2^{4q+3} - 1$. Nous donnons aussi celui du nombre $2^{19} - 1$ ; nous espérons donner ultérieurement ceux des nombres $2^{67} - 1$ et $2^{127} - 1$.

| 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | 0 |
| □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | 1 |
| □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | ■ | ■ | 2 |
| □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | 3 |
| □ | □ | □ | □ | □ | □ | □ | ■ | □ | □ | □ | ■ | □ | □ | ■ | ■ | ■ | ■ | ■ | 4 |
| □ | ■ | □ | □ | ■ | □ | ■ | □ | □ | ■ | □ | ■ | ■ | □ | □ | ■ | □ | □ | □ | 5 |
| ■ | □ | ■ | □ | ■ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | ■ | □ | ■ | □ | 6 |
| □ | ■ | ■ | ■ | □ | ■ | ■ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | □ | 7 |
| ■ | ■ | □ | □ | ■ | ■ | □ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | 8 |
| □ | □ | ■ | □ | ■ | □ | ■ | □ | □ | □ | □ | ■ | ■ | ■ | □ | □ | □ | □ | □ | 9 |
| ■ | □ | □ | ■ | ■ | ■ | ■ | ■ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | ■ | ■ | ■ | 10 |
| ■ | ■ | □ | □ | □ | ■ | ■ | ■ | ■ | □ | ■ | ■ | □ | ■ | ■ | □ | □ | ■ | □ | 11 |
| □ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | □ | □ | ■ | 12 |
| □ | ■ | □ | □ | □ | □ | □ | □ | ■ | ■ | □ | □ | □ | ■ | ■ | ■ | □ | □ | □ | 13 |
| ■ | ■ | ■ | □ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | ■ | □ | ■ | ■ | ■ | ■ | □ | 14 |
| ■ | ■ | □ | □ | □ | □ | ■ | ■ | □ | ■ | □ | □ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | 15 |
| ■ | ■ | □ | ■ | □ | ■ | ■ | □ | □ | ■ | ■ | □ | □ | □ | ■ | □ | ■ | □ | ■ | 16 |
| ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | □ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | 17 |
| □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | 18 |

DIAGRAMME DU NOMBRE PREMIER $2^{19} - 1$.

Lorsque l'on aura, par l'application du théorème fondamental, à vérifier de grands nombres premiers de la forme $\frac{3^n \pm 1}{3 \pm 1}$, on emploiera aussi avec succès le système ternaire, dans lequel on se servira seulement des chiffres 0, 1 et $\bar{1}$, à caractéristiques positives on négatives. Pour la vérification des grands nombres de la forme $10^{2^n} + 1$, on se servira facilement du système décimal, pour le calcul des résidus.

Lorsque le nombre essayé n'est pas premier, nous avons vu qu'on ne trouvera aucun résidu nul. Soit, par exemple, le nombre $p = 2^{11} - 1 = 2047$; les résidus que nous considérons sont, dans ce cas,

$$1, 3, 7, 47, 160, 1034, 620, -438, -576, 160, \ldots,$$

et se reproduisent périodiquement à partir de 160 suivant les cinq résidus

$$160, 1034, 620, -438, -576.$$

On peut donner une autre forme d'énoncé, au Théorème II, et aux suivants, en tenant compte des formules qui concernent les radicaux continus (Section XV); on a, par exemple:

THÉORÈME III : *Pour que le nombre* $p = 2^{4q+3} - 1$ *soit premier, il faut et il suffit que la congruence* $3 \equiv 2 \cos \frac{\pi}{2^{2q+1}}$, (Mod. $p$), *soit vérifiée, après la disparition successive des radicaux contenus dans la valeur du cosinus.* Nous démontrerons ultérieurement que cette condition est nécessaire et suffisante.

On observera encore que les nombres de la série

$$1, 3, 7, 47, 2207, \ldots\ldots$$

appartiennent tous, à partir du troisième, à la forme linéaire $5q + 2$; mais, d'autre part (Section VIII, Théor. II), les diviseurs de ces nombres appartiennent aux formes linéaires

$$20q + 1, 3, 7, 9;$$

par conséquent, chacun des termes de la série précédente contient un diviseur premier de la forme $5q + 2$; il en résulte immédiatement cette proposition :

THÉORÈME IV : *Il y a une infinité de nombres premiers appartenant à la forme linéaire* $5q + 2$.

On voit encore que les nombres de la série ont la forme $8h + 7$; mais, d'autre part, la forme des diviseurs quadratiques indique que les diviseurs de ces nombres sont de l'une des formes $8h + 1$, ou $8h + 7$; par conséquent, chacun des nombres de la série contient au moins un diviseur de la forme $8h + 7$, et, par suite :

THÉORÈME V : *Il y a une infinité de nombres premiers appartenant à la forme linéaire* $8h + 7$.

Les théorèmes suivants permettent d'arriver à un grand nombre de théorèmes analogues, qui sont des cas particuliers du théorème fondamental de LEJEUNE-DIRICHLET, sur la progression arithmétique. Nous devons observer, cependant, que les nombres de la forme $5q + 2$ ne sont pas tous compris dans la série que nous considérons ici, et qu'il en est de même dans tous les autres cas. Ainsi les théorèmes précédents diffèrent, au fond, des cas analogues de la progression arithmétique. La méthode que nous employons s'applique d'ailleurs, très-facilement, à la démonstration du théorème général suivant :

THÉORÈME VI : *Si A et Q désignent deux nombres quelconques premiers entre eux, la série*

$$r_0, r_1, r_2, r_3, \ldots\ldots r_n,$$

*dans laquelle on a*

$$r_0 = A\,,\quad r_1 = A^2 + 2Q\,,\quad r_{n+1} = r_n^2 - 2Q^{2^n}\,,$$

*contient comme diviseurs, des nombres premiers tous différents.*

Les formules de multiplication des fonctions numériques conduisent à des résultats analogues.

Par des considérations semblables aux précédentes, on démontrera les théorèmes suivants.

THÉORÈME VII: *Soit le nombre* $p = A\,.\,2^q - 1$, *et*

$$\left.\begin{array}{ll} 1^\circ, & q \equiv 0, \\ 2^\circ, & q \equiv 1, \\ 3^\circ, & q \equiv 2, \\ 4^\circ, & q \equiv 3, \end{array}\right\}\ (\text{Mod. } 4)\,,\quad \text{et}\quad \left.\begin{array}{lcl} A \equiv 3, & & \equiv 9, \\ A \equiv 7, & \text{ou} & \equiv 9, \\ A \equiv 1, & & \equiv 7, \\ A \equiv 1, & & \equiv 3, \end{array}\right\}\ (\text{Mod. } 10)\,;$$

*on forme les* $q$ *premiers termes de la série*

$$r_1,\ r_2,\ r_3,\ r_4,\ \ldots\ldots,$$

*par la relation de récurrence*

$$r_{n+1} = r_n^2 - 2\,,$$

*en prenant pour* $r_1$ *et* $r_2$ *les termes* $U_A$ *et* $V_A$, *de la série de* FIBONACCI. *Le nombre* $p$ *est premier, lorsque le rang du premier terme divisible par* $p$ *est égal à* $q$. *Si* $\alpha$ *désigne le rang du premier terme divisible par* $p$, *les diviseurs de* $p$ *sont de la forme* $2^\alpha.\,A\,.\,k \pm 1$, *combinée avec celle des diviseurs de* $x^2 - 2y^2$ *et de* $x^2 - 2Ay^2$.

THÉORÈME VIII: *On obtient un théorème semblable en prenant*

$$p = A\,.\,2^q + 1\,,$$

*avec les valeurs*

$$\left.\begin{array}{ll} 1^\circ, & q \equiv 0, \\ 2^\circ, & q \equiv 1, \\ 3^\circ, & q \equiv 2, \\ 4^\circ, & q \equiv 3, \end{array}\right\}\ (\text{Mod. } 4)\,,\quad \text{et}\quad \left.\begin{array}{lcl} A \equiv 5, & & \equiv 3, \\ A \equiv 5, & \text{ou} & \equiv 9, \\ A \equiv 5, & & \equiv 7, \\ A \equiv 5, & & \equiv 1, \end{array}\right\}\ (\text{Mod. } 10)\,;$$

soit, par exemple, $p = 3\,.\,2^{11} - 1 = 6143$. On forme la série des résidus

4, 18, 322, — 749, 1986, 388, 3110, 3016, 4614, 499, 0;

donc $p = 6143$ est premier.

THÉORÈME IX: *Soit le nombre*

$$p = A\,.\,3^q - 1\,,$$

*avec les valeurs*

$$\left.\begin{array}{ll} 1^\circ, & q \equiv 0, \\ 2^\circ, & q \equiv 1, \\ 3^\circ, & q \equiv 2, \\ 4^\circ, & q \equiv 3, \end{array}\right\}\ (\text{Mod. } 4)\,,\quad \text{et}\quad \left.\begin{array}{lcl} A \equiv 4, & & \equiv 8, \\ A \equiv 6, & \text{ou} & \equiv 8, \\ A \equiv 2, & & \equiv 6, \\ A \equiv 2, & & \equiv 4, \end{array}\right\}\ (\text{Mod. } 10)\,;$$

*on forme les q premiers termes de la série*

$$r_1, r_2, r_3, \ldots,$$

*par la formule de récurrence*

$$r_{n+1} = r_n^3 + 3r_n^2 - 3,$$

*déduite des formules de triplication, avec les conditions initiales*

$$r_0 = U_A, \; r_1 = \frac{U_{3A}}{U_A},$$

*dans la série de* FIBONACCI; *le nombre p est premier lorsque le rang du premier terme divisible par p est égal à q; si α désigne le rang du premier terme divisible par p, les diviseurs de p sont de la forme* $3^\alpha . A . k \pm 1$, *combinée avec celle des diviseurs quadratiques correspondants.*

EXEMPLE: Pour $p = 2 . 3^7 - 1$, les résidus sont

2, 17, 1404, 0;

donc $p = 4373$ est un nombre premier, puis qu'il n'a pas de diviseur inférieur à sa racine carrée.

THÉORÈME X: *On a un théorème analogue en supposant*

$$p = A . 3^q + 1,$$

*avec les valeurs*

$$\left.\begin{matrix} q \equiv 0, \\ q \equiv 1, \\ q \equiv 2, \\ q \equiv 3, \end{matrix}\right\} \text{(Mod. 4)}, \quad \text{et} \quad \left.\begin{matrix} A \equiv 0, \\ A \equiv 0, \\ A \equiv 0, \\ A \equiv 0, \end{matrix} \quad \text{ou} \quad \begin{matrix} \equiv 8, \\ \equiv 6, \\ \equiv 2, \\ \equiv 4, \end{matrix}\right\} \text{(Mod. 10)};$$

*et la relation de récurrence*

$$r_{n+1} = r_n^3 - 3r_n^2 + 3.$$

EXEMPLE: Pour $p = 2 . 3^6 + 1$, on a les résidus

4, 19, — 57, 569, — 212, 0;

donc $p = 1459$ est premier.

THÉORÈME XI: *Soit le nombre*

$$p = 2A . 5^q + 1;$$

*on forme la série limitée à q termes*, $r_0, r_1, r_2, r_3, \ldots,$

*par la relation de récurrence*

$$r_{n+1} = r_n^5 + 5r_n^3 + 5r_n,$$

*et les conditions initiales*

$$r_0 = U_A, \; r_1 = U_{5A},$$

*dans la série de* FIBONACCI; *le nombre p est premier, lorsque le rang du premier terme divisible par p est égal à q; il est composé, si aucun des q termes n'est divisible par p; enfin, si α désigne le rang du premier résidu nul, les diviseurs premiers de p sont de l'une des formes* $2A . 5^\alpha k \pm 1$.

## SECTION XXVIII.

*Sur la division géométrique de la circonférence en parties égales.*

Dans la section précédente, nous n'avons considéré que la vérification des nombres premiers par l'emploi de la série de FIBONACCI; il est clair que toutes les autres séries donnent lieu à de semblables théorèmes; par suite de l'indétermination laissée à la somme $P$ et au produit $Q$ des deux racines de l'équation fondamentale, on pourra toujours s'assurer du mode de composition d'un nombre $p$, lorsque l'on connaîtra l'une ou l'autre des decompositions de $p+1$ ou de $p-1$, en facteurs premiers. Nous donnerons encore l'application du théorème fondamental, aux nombres premiers dans lesquels on peut diviser géométriquement la circonférence, en parties égales.

La théorie de la division géomètrique de la circonférence, en parties égales, a été donnée par GAUSS, dans la dernière section des *Disquisitiones Arithmeticæ.* Il est convenu que cette opération ne peut être exécutée que des trois maniéres suivantes: 1° par l'emploi simultané de la règle et du compas, comme dans la construction ordinaire du décagone régulier (EUCLIDE); 2° par l'emploi du compas sans la règle (MASCHERONI); 3° par l'emploi de la double règle, sans compas, c'est-à-dire d'une règle plate dont les deux bords sont rectilignes et parallèles. Cette idée ingénieuse est due à M. DE COATPONT, colonel du génie.

GAUSS a démontré que, pour diviser géométriquement la circonférence en $N$ parties égales, il faut et il suffit que

$$N = 2^{\mu} \,.\, a_i \,.\, a_j \,.\, a_k \,.\,.\,.\,.\,,$$

$\mu$ étant arbitraire, $a_i$, $a_j$, $a_k$, .... des nombres premiers et différents, en nombre quelconque, mais de la forme

$$a_n = 2^{2^n} + 1\,.$$

On a, pour les premières valeurs de $n$,

$$a_0 = 3\,,\; a_1 = 5\,,\; a_2 = 17\,,\; a_3 = 257\,,\; a_4 = 65537\,;$$

mais $a_5$ est divisible par 641 (Section XXVI), et ne peut être compris dans l'expression de $N$. Il reste donc deux questions importantes à résoudre: 1° comment peut-on s'assurer que $a_n$ est premier? 2° existe-t-il une série indéfinie de nombres premiers $a_n$? Nous ne répondrons, pour l'instant, qu'à la première question.

Si $a_n$ est premier, le nombre $Q$ est résidu quadratique de $a_n$; donc, dans la série de PELL, $V_{a_n - 1}$ est divisible par $a_n$; mais $a_n - 1$ a pour diviseurs les nombres,

$$2, 2^2, 2^3, \ldots . 2^n;$$

on a donc, par l'application du théorème fondamental, et par les formules de duplication, le théorème suivant:

THÉORÈME I: *Soit le nombre* $a_n = 2^{2^n} + 1$; *on forme la série des* $2^n - 1$ *termes,*

$$6, 34, 1154, 13\,31714, 17\,73462\,17794, \ldots,$$

*tels que chacun d'eux est égal au carré du précédent diminué de deux unités; le nombre* $a_n$ *est premier, lorsque le premier terme divisible par* $a_n$ *est compris entre les termes de rang* $2^{n-1}$ *et* $2^n - 1$; *il est composé, si aucun des termes de la série n'est divisible par* $a_n$; *enfin si* $\alpha < 2^{n-1}$ *désigne le rang du premier terme divisible par* $a_n$, *les diviseurs premiers de* $a_n$ *appartiennent à la forme linéaire*

$$2^{2^{\alpha+1}} . q + 1 .$$

On obtiendrait un théorème analogue pour l'essai des grands nombres premiers de la forme $A . 2^{2^n} + 1$.

Le savant P. PÉPIN a présenté à l'Académie des Sciences de Paris (*Comptes rendus*, 6 Août 1877), un autre théorème pour reconnaître les nombres premiers $a_n$, qui rentre dans notre méthode générale. En effet, au lieu de nous servir de la série de PELL, nous pouvons employer beaucoup d'autres séries récurrentes, et ainsi la série récurrente de première espèce, dont les termes sont donnés par l'expression

$$U_r = \frac{a^r - b^r}{a - b},$$

dans laquelle $a$ et $b$ désignent deux nombres entiers arbitraires. En faisant $b = 1$ et $a$ quelconque, on obtiendra un théorème analogue au précédent; mais si, de plus, par la loi de réciprocité des résidus quadratiques, on choisit pour $a$ un non-résidu de $a_n$ supposé premier, $a = 5$, par exemple, il est clair que le rang du premier résidu nul sera exactement égal à $2^n - 1$. De cette façon, la forme ambigüe donnée à l'énoncé de nos théorèmes disparaît, il est vrai, et l'on obtient alors une *condition nécessaire et suffisante* pour que $a_n$ soit premier. Il serait facile de tenir compte de cette observation, et de donner une série de théorèmes analogues, dans la recherche de la condition nécessaire et suffisante pour qu'un nombre $2^n \alpha p \pm 1$ soit premier, lorsque $\alpha$ désigne un produit de facteurs premiers donnés, et $p$ un nombre premier arbitraire. On a, par exemple, les théorèmes suivants.

Théorème II: *Lorsque* $p = 10q + 7$ *ou* $p = 10q + 9$ *est un nombre premier, le nombre* $2p - 1$ *est premier si l'on a, dans la série de* Fibonacci,

$$U_p \equiv 0, \quad (\text{Mod. } 2p - 1),$$

*et réciproquement.*

Théorème III: *Lorsque* $p = 4q + 3$ *est un nombre premier, le nombre* $2p + 1$ *est premier si l'on a, dans la série de* Fermat,

$$U_p \equiv 0, \quad (\text{Mod. } 2p + 1),$$

*et réciproquement.*

Théorème IV: *Lorsque* $p = 4q + 3$ *est un nombre premier, le nombre* $2p - 1$ *est premier si l'on a, dans le série de* Pell,

$$U_p \equiv 0, \quad (\text{Mod. } 2p - 1),$$

*et réciproquement.*

On doit cependant observer que si la méthode indiquée par le P. Pépin, conduit à une forme plus claire et plus précise de l'ènoncé, qui devient ainsi semblable à celui du théorème de Wilson, il est préférable de s'en tenir, dans l'application, à la forme que nous avons adoptée. En effet, l'application de ces théorèmes repose sur une hypothèse, celle de considérer comme premier un nombre pris arbitrairement dans une certaine forme; il est plus probable de supposer, au contraire, le nombre comme composé, ainsi que semble l'indiquer l'assertion du P. Mersenne. Par conséquent, au lieu de reculer la vérification, jusqu'à l'extrême limite, par l'emploi des non-résidus quadratiques, il serait plus pratique, dans l'exemple, de se servir de l'un des $\phi(2^{n-1})$ nombres qui appartiennent à l'exposant $2^{n-1}$, pour le module $a_n$ supposé premier; mais cette recherche directe est fort difficile. On s'assurera cependant que, par le théorème I, il suffit, pour démontrer que $a_2$, $a_3$, $a_4$, sont premiers, d'exécuter respectivement 3, 6, 12, opérations au lieu du nombre 4, 8, 16, qui lui correspond dans l'autre méthode.

## Section XXIX.

### *Sur la vérification de l'assertion du* P. Mersenne.

Nous avons indiqué la marche à suivre pour les nombres de la forme $2^{4q+3} - 1$; il nous reste à indiquer une marche analogue pour les nombres de la forme $p = 2^{4q+1} - 1$, tels que

$$2^{61} - 1, 2^{97} - 1, \ldots, 2^{257} - 1.$$

En supposant $p$ premier, $-1$ est non-résidu de $p$ puisque $p$ est de la forme $4k+3$, et 2 est résidu de $p$, puisque $p$ est de la forme $8k+7$; donc $-2$ est non-résidu de $p$. Par conséquent, la série conjuguée de celle de PELL, c'est-à-dire la série provenant de l'équation,

$$x^2 = 2x + 3,$$

dans laquelle

$$P = 2, \quad Q = -3, \quad \Delta = 2^2 \times (-2),$$

est propre à la vérification des nombres premiers que nous considérons, puisque, si $p$ est premier, $U_{p+1}$ est divisible par $p$. Les diviseurs de $p+1$ représentent toutes les puissances de 2 jusqu'à l'exposant $4q+1$; il suffira donc de calculer les résidus de

$$U_1, \; V_1, \; V_2, \; V_4, \ldots \; V_{2^{4q}},$$

par les formules ordinaires de duplication.

Mais nous devons encore faire une observation importante, au point de vue du calcul. Puisque l'on emploie la formule

$$V_{2^{\lambda+1}} = (V_{2^\lambda})^2 - 2Q^{2^\lambda},$$

il est bon, si l'on effectue le calcul des résidus dans le système de numération décimale, de supposer $Q = \pm 1$, ou $Q = \pm 10^n$; car sans cela, on double la longueur des calculs, ainsi qu'il est facile de s'en apercevoir; si l'on opère dans le système de numération binaire, il sera commode de supposer $Q$ égal, en valeur absolue, à l'unité ou à une puissance de 2.

Il est donc préférable d'employer la série récurrente provenant de l'équation

$$x^2 = 4x - 1,$$

dans laquelle

$$a = 2 + \sqrt{3}, \qquad b = 2 - \sqrt{3},$$

et

$$P = 4, \qquad Q = 1, \qquad \Delta = 2^2 \times 3.$$

En supposant que $p = 2^{4q+1} - 1$ est un nombre premier, on a, par la loi de réciprocité,

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right),$$

puisque $p$ et 3 sont tous deux des multiples de 4 plus 3; d'autre part, par le théorème de FERMAT

$$2^{4q+1} - 1 \equiv 1, \quad (\text{Mod. } 3);$$

donc 3 est non-résidu de $p$, supposé premier, et, dans ce cas, $U_{p+1}$ est divisible par $p$. Les diviseurs de $p+1$ sont égaux à toutes les puissances de 2 jusqu'à $4q+1$, et, de plus, $Q = 1$.

Par conséquent, on formera la suite des résidus

$$4, 14, 194, 37634, \ldots .$$

tels que chacun d'eux est égal au carré du précédent diminué de deux unités.

EXEMPLE: Soit le nombre $2^{13} - 1 = 8191$; on trouve les résidus

$$4, 14, 194, 4870, 3953, 5970, 1857, 36, 1294, 3470, 128, 0;$$

donc le nombre $2^{13} - 1$ est premier.

On a donc le théorème suivant:

THÉORÈME: *Soit le nombre $p = 2^{4q+1} - 1$; on forme la série des résidus*

$$4, 14, 194, 37634, \ldots ,$$

*tels que chacun d'eux est égal au carré du précédent diminué de deux unités; le nombre p est composé, si aucun des $4q + 1$ premiers résidus n'est égal à 0; le nombre p est premier si le premier résidu nul occupe un rang compris entre $2q$ et $4q + 1$; si le rang du premier résidu est égal à $\alpha < 2q$, les diviseurs de p appartiennent à la forme linéaire*

$$2^{\alpha+1}k + 1.$$

On aurait encore des théorèmes analogues pour les nombres de la forme

$$A \,.\, 2^{4q+1} - 1.$$

Avant de terminer ce paragraphe, nous ferons observer que nous pensons n'avoir qu'effleuré le sujet qui nous occupe. Il reste à trouver, comme pour les nombres premiers, un criterium des nombres composés, affranchi de l'incertitude des calculs numériques; dans un grand nombre de cas, lorsque le nombre essayé n'est pas premier, il se présente une période dans la suite des résidus; mais, s'il est vrai, comme nous l'avons démontré (Section XXVI), que cette période existe, lorsque l'on considére l'ensemble des résidus de tous les termes de la série récurrente, il n'est pas démontré que cette période se manifestera, si l'on ne considére qu'un certain nombre d'entre eux, dont les rangs sont en progression géométrique. C'est là un problème important à résoudre.

En second lieu, lorsque l'ensemble des calculs démontre que le nombre essayé n'est pas premier, peut-on arriver facilement, par la connaissance de la série des rèsidus calculés, à la décomposition du nombre que l'on avait supposé premier? Ces résidus forment, comme nous l'avons dit, un fragment d'un *Canon Arithmeticus généralisé*, que l'on peut comparer aux tables des logarithmes des sinus et des cosinus, ainsi que l'on compare le Canon Arithmeticus lui-même, aux tables des logarithmes des nombres. C'est là un second problème à résoudre.

Nous avons encore indiqué (Sections IX et XXI), une première généralisation de l'idée principale de ce mémoire, dans l'étude des séries récurrentes qui naissent des fonctions symétriques des racines des équations algébriques du troisième et du quatrième degré, et, plus généralement, des racines des équations de degré quelconque, à coefficients commensurables. On trouve, en particulier, dans l'étude de la fonction.

$$U_n = \frac{\Delta\,(a^n\,,\, b^n\,,\, c^n\,, \ldots.)}{\Delta\,(a\,,\, b\,,\, c\,, \ldots.)}\,,$$

dans laquelle $a$, $b$, $c$, .... désignent les racines de l'équation, et $\Delta\,(a, b, c, \ldots.)$ la *fonction alternée* des racines, ou la racine carrée du discriminant de l'équation, la généralisation des principales formules contenues dans la première partie de ce travail.

Enfin, il reste à développer la théorie de la division des fonctions numériques, et son application à l'analyse indéterminée du second degré et des degrés superieurs; c'est une étude que nous espérons publier prochainement. Nous donnons d'ailleurs, dans le dernier paragraphe qui suit, une autre généralisation des fonctions numériques périodiques, déduite de la considération des séries ordonnées suivant les puissances de la variable.

## SECTION XXX.

*Sur la périodicité numérique des coefficients différentiels des fonctions rationnelles d'exponentielles.*

L'étude des nombres premiers contenus dans les dénominateurs des coefficients des puissances de la variable, dans les développements en séries, lorsque l'on suppose ces coefficients réduits à leur plus simple expression, a conduit EISENSTEIN à la découverte d'un théorème remarquable. En effet, ce théorème fournit un criterium qui permet de décider, à la seule inspection des facteurs premiers du dénominateur, si la fonction qui représente la somme de la série supposée convergente, est *algébrique* ou *transcendante*.

On sait encore que l'étude des facteurs premiers contenus dans les numérateurs des coefficients $B_n$ de $\dfrac{z^n}{1\,.\,2\,.\,3\ldots n}$ dans le développement de $\dfrac{z}{1-e^z}$, ou, en d'autres termes, dans les numérateurs des *nombres de* BERNOULLI, a conduit CAUCHY, MM. GENOCCHI et KUMMER, à d'importants résultats sur la théorie des résidus quadratiques, et sur celle de l'équation indéterminée

$$x^p + y^p + z^p = 0\,,$$

dont FERMAT a affirmé l'impossibilité en nombres entiers, pour $p > 2$. Ainsi M. KUMMER a démontré que cette équation ne peut être vérifiée par des nombres entiers, lorsque $p$ ne se trouve pas comme facteur dans les numérateurs des nombres de BERNOULLI $B_2$, $B_4$, $B_6$, . . . $B_{p-3}$.*

En se plaçant à un point de vue différent, MM. CLAUSEN et STAUDT ont donné pour ces nombres cette expression remarquable

$$B_{2n} = A_{2n} - \frac{1}{2} - \frac{1}{\alpha} - \frac{1}{\beta} - \dots - \frac{1}{\lambda},$$

dans laquelle $A_{2n}$ est un nombre entier, et les dénominateurs $2, \alpha, \beta, \gamma, \dots \lambda$, tous les nombres premiers qui surpassent d'une unité tous les diviseurs de $2n$. Cette formule conduit au procédé le plus rapide pour le calcul de ces nombres; M. ADAMS vient de donner, par son emploi, les valeurs des 62 premiers nombres (*British Association*,—Plymouth, Août 1877.)

Nous avons indiqué aussi comment l'application combinée des théorèmes de FERMAT et de STAUDT conduit à cette propriété que les nombres

$$a\,(a^{2n} - 1)\,B_{2n},$$

sont entiers, quel que soit l'entier $a$. Nous allons montrer que l'étude des coefficients de $\dfrac{x^n}{1.2.3\dots n}$ dans le développement des fonctions rationnelles d'exponentielles, ou, en d'autres termes, les coefficients différentiels de ces fonctions, pour $x = 0$, conduit à des propriétés importantes.

On sait, en effet, que si l'on remplace $x$ par les nombres entiers consécutifs dans la fonction

$$\phi\,(x) = Aa^x + Bb^x + Cc^x + Dd^x + \dots$$

dans laquelle $A, B, C, D, \dots$ et $a, b, c, d, \dots$ sont entiers, on a, pour $p$ premier et $k$ entier quelconque, la congruence

$$(148) \qquad \phi\,[x + k\,(p-1)] \equiv \phi\,(x)\,, \quad (\text{Mod.}\,p).$$

Nous avons étendu cette propriété aux fonctions numériques $U_n$ et $V_n$; il est facile de voir que cette proposition s'applique aux coefficients différentiels d'une fonction entière de $e^x$ et de $e^{-x}$. Il nous reste à montrer que cette

---

*Nous avons modifié les diverses notations qui concernent ces nombres. La présente notation se prête beaucoup plus facilement aux développements que comporte la théorie de ces nombres. Voir, sur ce sujet, les Notes insérées dans les *Comptes rendus de l'Académie des Sciences de Paris* (Septembre 1876), dans les *Annali di Matematica* (2e série, tome VIII), dans les *Nouvelles Annales de Mathématiques* (2e série, tome XVI, pag. 157), dans la *Nouvelle Correspondance Mathématique* (tome II, pag. 328, et tome III, pag. 69), dans *The Messenger of Mathematics*, (Octobre 1877), etc.

proposition s'applique encore aux coefficients différentiels d'une fonction rationnelle de $e^x$ et de $e^{-x}$.

Soit d'abord

(149) $$\text{séc}\, x = 1 + a_2 x^2 + a_4 x^4 + a_6 x^6 + \ldots ;$$

M. SYLVESTER a appelé *nombres Eulériens* (*Comptes rendus*, t. LII, pag. 161), les coefficients, pris en valeur absolue, déterminés par la relation

(150) $$E_{2n} = (-1)^n\, 1, 2, 3 \ldots (2n)\; Q_{2n} ;$$

on a, par le changement de $x$ en $x\sqrt{-1}$, la formule symbolique

(151) $$u = \frac{2}{e^x + e^{-x}} = e^{Ex},$$

dans laquelle on remplacera, dans le développement du second membre les exposants de $E$ par des indices; ainsi

$$\frac{d^n u_0}{dx_0^{\,n}} = E_n .$$

En chassant les dénominateurs de l'identité (151), on obtient, par l'identification des coefficients de $x^n$, la formule

(152) $$(E+1)^n + (E-1)^n = 0,$$

qui permet de calculer les nombres Eulériens par voie récurrente. On a aussi le déterminant

(153) $$E_{2n} = (-1)^n \begin{vmatrix} 1 & 1 & 0 & 0 & . & . & . & . & 0 \\ 1 & 6 & 1 & 0 & . & . & . & . & 0 \\ 1 & 15 & 15 & 1 & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & 0 \\ 1 & C_{2n}^2 & C_{2n}^4 & C_{2n}^6 & . & . & . & . & C_{2n}^2 \end{vmatrix};$$

ce déterminant est formé par les lignes de rang pair et les colonnes de rang impair du triangle arithmétique. Les nombres Eulériens sont entiers et impairs; SHERK a démontré qu'ils sont terminés alternativement par les chiffres 1 et 5*. Ces propriétés sont des cas particuliers des suivantes.

En tenant compte des résultats obtenus (Section XXI), sur les congruences du triangle arithmétique, la formule (152) donne, pour $p$ premier, et $n = p - 1$,

(154) $$E_{p-1} + E_{p-3} + E_{p-5} + \ldots + E_2 + E_0 \equiv 0, \quad (\text{Mod.}\, p);$$

on a donc cette proposition:

---

* *Journal de Crelle*, t. 79, pag. 67.

THÉORÈME: *Si $p$ est un nombre premier, la somme des nombres Eulériens, pris avec les signes alternés $+$ et $-$, dont l'indice est plus petit que $p$, est divisible par $p$.*

Les premières valeurs de $E$ sont donnés par les relations

$$E_2 + E_0 = 0\,,$$
$$E_4 + 6E_2 + E_0 = 0\,,$$
$$E_6 + 15E_4 + 15E_2 + E_0 = 0\,,$$
$$\cdots\cdots\cdots\,,$$
$$\cdots\cdots\cdots\,;$$

on a ensuite, par congruence, à partir de $E_{p+1}$, pour le module premier $p$

$$E_{p+1} + E_0 \equiv 0\,,$$
$$E_{p+3} + 3E_{p+1} + 3E_2 + E_0 \equiv 0\,,$$
$$E_{p+5} + 10E_{p+3} + 5E_{p+1} + 5E_4 + 10E_2 + E_0 \equiv 0\,,$$
$$\cdots\cdots\cdots\,,$$
$$\cdots\cdots\cdots\,;$$

la comparaison des deux groupes de formules qui précédent, donne successivement

(155)
$$E_{p+1} \equiv E_2\,, \quad (\text{Mod. } p)\,,$$
$$E_{p+3} \equiv E_4\,, \quad \text{“}$$
$$E_{p+5} \equiv E_6\,, \quad \text{“}$$
$$\cdots\cdots\cdots$$

On obtient de même, en général, pour $k$ entier quelconque

(156) $$E_{2n+k(p-1)} \equiv E_{2n}\,, \quad (\text{Mod. } p)\,,$$

et, par suite:

THÉORÈME: *Les résidus des nombres Eulériens, suivant un module premier quelconque, se reproduisent périodiquement dans le même ordre, comme les résidus des puissances des nombres entiers.*

Posons maintenant

$$u^{\alpha} = \left(\frac{2}{e^x + e^{-x}}\right)^{\alpha} = E_{\alpha,0} + E_{\alpha,1}\frac{x}{1} + E_{\alpha,2}\frac{x^2}{1\,.\,2} + \cdots + E_{\alpha,n}\frac{x^n}{1\,.\,2\ldots n} + \cdots$$

ou, sous la forme symbolique

(157) $$u^{\alpha} = e^{E_{\alpha}x}\,,$$

les coefficients $E_{\alpha,n}$ sont déterminés par la relation symbolique

(158) $$E_{\alpha,n} = [E' + E'' + E''' + \ldots + E^{(\alpha)}]^n\,,$$

dans le développement de laquelle on remplace les exposants de $E', E'', \ldots E^{(\alpha)}$ par des indices, et en supprimant les accents. On a aussi la formule

(159) $$E_{\alpha, n} = [E_{\alpha-1} + E_1]^n,$$

dans laquelle en remplace les exposants de $E_{\alpha-1}$ et de $E_1$ par des seconds indices. Ces nombres $E_{\alpha, n}$ que nous appellerons les *nombres Eulériens d'ordre* $\alpha$ sont entiers pour $\alpha$ entier et positif; on démontre, comme ci-dessus, que leurs résidus suivant un module premier se reproduisent périodiquement, et que l'on a encore

(160) $$E_{\alpha, n} \equiv E_{\alpha, n+k(p-1)}, \quad (\text{Mod. } p).$$

Ces considérations s'appliquent, en général, aux coefficients différentiels d'une fraction rationnelle de $e^x$, mais, dans certaines conditions, comme dans le cas de

$$\frac{\phi(1)}{\phi(e^x)}.$$

Cependant, lorsque $\phi(1)$ est nul, comme dans le développement de $\frac{1}{1-e^x}$ qui contient les nombres de BERNOULLI, ce théorème ne se présente plus immédiatement, puisque les coefficients ne sont plus entiers, et contiennent en dénominateur une série indéfinie de nombres premiers. Alors, on les multiplie par d'autres fonctions telles que

$$a(a^n - 1)$$

afin de les rendre entiers, et d'appliquer les résultats qui proviennent des congruences du triangle arithmétique.

PARIS, Décembre, 1877.